WHAT IS CLAIMED IS:

1. A data processor which is supplied with command data specifying a data component to be used for controlling itself, and operates based on said command data, said data processor comprising:

transmission/reception means for transmitting/receiving data to/from a server connected over a network;

validity determination means for determining whether said command data is valid;

command data processing means for retrieving, when said command data is determined as valid by said validity determination means, the data component specified by said command data from said server using said transmission/reception means; and

data component processing means for controlling said data processor based on the data component retrieved by said command data processing means.

2. The data processor according to claim 1, wherein said data component processing means performs screen display based on the data component retrieved by said command data processing means.

3. The data processor according to claim 1, wherein

said data component processing means outputs the data component retrieved by said command data processing means to outside of said data processor.

4. The data processor according to claim 1, wherein the data component used for controlling said data processor by said data component processing means is limited to be the data component retrieved by said command data processing means.

5. The data processor according to claim 1, wherein

said command data is encrypted, and

said validity determination means determines whether said command data is valid after decrypting the same.

6. The data processor according to claim 1, wherein said command data processing means determines whether the data component retrieved from said server is valid, and if determined valid, supplies the data component to said data component processing means.

7. The data processor according to claim 1, wherein said command data processing means includes a language processing section for interpreting a JAVA language, and a JAVA applet to be processed by said language processing section.

8. The data processor according to claim 7, wherein said transmission/reception section receives, in accordance with a user's instruction, the JAVA applet included in said command data processing means.

9. The data processor according to claim 1, wherein said transmission/reception means receives, in accordance with a user's instruction, said command data for supply to said validity determination means.

10. A data processor which is supplied with command data including a data component used for controlling itself, and operates based on said command data, said data processor comprising:

transmission/reception means for transmitting/receiving data to/from a server connected over a network;

validity determination means for determining whether said command data is valid;

command data processing means for retrieving, when said command data is determined as valid by said validity determination means, the data component included in said command data; and

data component processing means for controlling said data processor based on the data component retrieved by said command data processing means.

11. The data processor according to claim 10, wherein said data component processing means performs screen display based on the data component retrieved by said command data processing means.

12. The data processor according to claim 10, wherein said data component processing means outputs the data component retrieved by said command data processing means to outside of said data processor.

13. The data processor according to claim 10, wherein the data component used for controlling said date processor by said data component processing means is limited to be the data component retrieved by said command data processing means.

14. The data processor according to claim 10, wherein

said command data is encrypted, and

said validity determination means determines whether said command data is valid after decrypting the same.

15. The data processor according to claim 10, wherein said command data processing means includes a language processing section for interpreting a JAVA language, and a JAVA applet to be processed by said language processing section.

16. The data processor according to claim 15, wherein said transmission/reception section receives, in accordance with a user's instruction, the JAVA applet included in said command data processing means.

17. The data processor according to claim 10, wherein said transmission/reception means receives, in accordance with a user's instruction, said command data for supply to said validity determination means.

18. A data processing method in which command data specifying a data component to be used for controlling a data processor is supplied, and said command data is used as a basis for an operation, said method comprising:

a transmission/reception step of transmitting/receiving data to/from a server connected over a network;

a validity determination step of determining whether said command data is valid;

a command data processing step of retrieving, when said command data is determined as valid in said validity determination step, the data component specified by said command data from said server by calling for said transmission/reception step; and

a data component processing step of controlling said data processor based on the data component retrieved in said

command data processing step.

19. A data processing method in which command data including a data component used for controlling a data processor is supplied, and said command data is used as a basis for an operation, said method comprising:

a transmission/reception step of transmitting/receiving data to/from a server connected over a network;

a validity determination step of determining whether said command data is valid;

a command data processing step of retrieving, when said command data is determined as valid in said validity determination step, the data component included in said command data; and

a data component processing step of controlling said data processor based on the data component retrieved in said command data processing step.

20. A data processor for receiving and processing data to which information for tampering detection is added, said data processor comprising:

reception means for receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data

region for including data not to be subjected to tampering detection, wherein said protected data region includes an unprotection list which lists, by type, the data included in said unprotected data region ;

protected data authentication means for detecting, for the data received by said reception means, whether the data included in said protected data region has been tampered by using the tampering detection information included in said authentication information region; and

unprotected data authentication means for authenticating, for the data received by said reception means, whether the data included in said unprotected data region is valid based on said unprotection list which has been confirmed as not having been tampered by said protected data authentication means.

21. The data processor according to claim 20, wherein the data received by said reception means is hypertext, and

said unprotection list lists, by type, a tag included in said unprotected data region.

22. A data processor structured by a transmitting data processor and a receiving data processor, wherein the transmitting data processor transfers, to the receiving data processor, data to which information for tampering detection is

added, wherein

said transmitting data processor comprises:

unprotection list generation means for generating an unprotection list which lists, by type, data not to be subjected to tampering detection;

data generation means for generating data to be transmitted by arranging data to be subjected to tampering detection in a protected data region together with said unprotection list, the data not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in said protected data region in an authentication information region; and

transmission means for transmitting the data generated by said data generation means, and

said receiving data processor comprises:

reception means for receiving the data transmitted from said transmitting data processor;

protected data authentication means for detecting, for the data received by said reception means, whether the data in said protected data region has been tampered by using the tampering detection information in said authentication information region; and

unprotected data authentication means for authenticating, for the data received by said reception means, whether the data included in said unprotected data region is valid

based on said unprotection list which has been confirmed as not having been tampered by said protected data authentication means.

23. The data processor according to claim 22, wherein

the data generated by said data generation means is hypertext, and

said unprotection list lists, by type, a tag included in said unprotected data region.

24. A data processing method for receiving and processing data to which information for tampering detection is added, said method comprising:

a reception step of receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data not to be subjected to tampering detection, wherein said protected data region includes an unprotection list which lists, by type, the data included in said unprotected data region;

a protected data authentication step of detecting, for the data received in said reception step, whether the data included in said protected data region has been tampered by using the tampering detection information included in said authentication information region; and

an unprotected data authentication step of authenticating, for the data received in said reception step, whether the data included in said unprotected data region is valid based on said unprotection list which has been confirmed as not having been tampered in said protected data authentication step.

25. A data processing method for transferring data to which information for tampering detection is added from a transmitting data processor to a receiving data processor, wherein

said transmitting data processor performs:

an unprotection list generation step of generating an unprotection list which lists, by type, data not to be subjected to tampering detection;

a data generation step of generating data to be transmitted by arranging data to be subjected to tampering detection in a protected data region together with said unprotection list, the data not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in said protected data region in an authentication information region; and

a transmission step of transmitting the data generated in said data generation step, and

said receiving data processor performs:

a reception step of receiving the data transmitted

from said transmitting data processor;

a protected data authentication step of detecting, for the data received in said reception step, whether the data in said protected data region has been tampered by using the tampering detection information in said authentication information region; and

an unprotected data authentication step of authenticating, for the data received in said reception step, whether the data included in said unprotected data region is valid based on said unprotection list which has been confirmed as not having been tampered in said protected data authentication step.

26. A data processor for receiving and processing data with a digital signature, comprising:

reception means for receiving the data with the digital signature from a server connected over a network;

signer certificate acquiring means for acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received by said reception means; and

signature authentication means for determining, when the signer certificate acquired by said signer certificate acquiring means indicates, by type, the data received by said reception means, that a signature applied to the data as valid.

27. The data processor according to claim 26, wherein

said signer certificate can include, in a list, by type, a plurality of the signable data.

28. The data processor according to claim 26, wherein said signer certificate can include a wildcard as a type of the signable data, and

when the signer certificate acquired by said signer certificate acquiring means includes the wildcard as the type of the signable data, said signature authentication means determines that the signature applied to any data received in said reception means as valid.

29. The data processor according to claim 26, wherein said signature authentication means acquires a type of the data based on a characteristic part of a URI (Uniform Resource Identifier) of the data received by said reception means.

30. The data processor according to claim 26, wherein said signature authentication means acquires the type of the data based on a header part of the data received by said reception means.

31. The data processor according to claim 26, wherein said signer certificate acquiring means receives said signer certificate by using said reception means.

32. A data processing method for receiving and processing data with a digital signature, comprising:

a reception step of receiving the data with the digital signature from a server connected over a network;

a signer certificate acquiring step of acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received in said reception step; and

a signature authentication step of determining, when the signer certificate acquired in said signer certificate acquiring step indicates, by type, the data received in said reception step, that a signature applied to the data as valid.